REMARKS

The specification has been amended to make editorial changes therein.

Claims 1, 17, 37, and 49 have been amended and claims 33-36 and 45-48 have been canceled.

The Official Action objects to the form of claims 13-15, which have been amended by making them depend from claim 12 as suggested in the Official Action. Reconsideration and withdrawal of the objection are respectfully requested.

Claims 45-48 and 49-56 were rejected under 35 U.S.C. 101. Claims 45-48 have been canceled and claims 49-56 have been amended by defining the program as stored in a computer readable-medium and comprising computer executable instructions as suggested in the Official Action. Reconsideration and withdrawal of the rejection are respectfully requested.

Claims 1-56 were rejected as unpatentable over GB 2 360 107 in view of O'DONNELL et al. 7,117,529. Reconsideration and withdrawal of the rejection of claims 1-32, 37-44, and 49-56 are respectfully requested.

The amended claims provide, among other features, that authentication is based solely on the user authentication information from the server device and without regard for prior authentication information in the client device. Support for the amendment is found, for example, at page 34, lines 18-22; page 35, line 9 through page 36, line 15; and Figures 4-5 and 10.

While the exact words of the amendment do not appear in the specification, it is believed that the amendment accurately reflects what one of skill in the art would learn from the specification when considered in its entirety.

As explained below, the references do not disclose or suggest that authentication when opening a maintenance interface in the client device is to be based solely on the input from the server without regard for prior authentication information. In the prior art, the authentication is commenced by a permission request from a client device, not on the information from the server (e.g., GB'107 Figure 13, element 1310 and page 21, lines 9-21).

GB'107 describes a framework by which security policy and application guards are distributed from a policy manager located in a server. The reference does not disclose that permission to open a maintenance interface at a client device can be carried out from a maintenance console of a server. In GB'107 a series of actions are commenced by a permission request from a client device. By contrast, in the present invention, actuation of a maintenance console at a client device is enabled by permission given from the maintenance console of a server regardless of the permission request from the client device.

O'DONNELL et al. describe a system in which a user is able to dynamically grant or deny permission for a technical support representative to access the user's data. There is no

mention of having the technical support representative access the user's data based on authentication information from a server (regardless of permission from the client device).

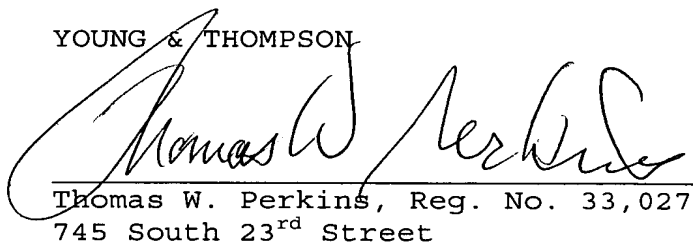
With regard to claims 17 and 49, in GB'107 the server includes a GUI for executing the security settings of the client devices and records and manages information of the client devices in the server. By contrast, in these methods the maintenance staff executes settings and management via the server from the console on the server side. O'DONNELL et al. do not disclose steps (c) and (d) of these claims.

In view of the present amendment and the foregoing remarks, it is believed that the present application has been placed in condition for allowance. Reconsideration and allowance are respectfully requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON



Thomas W. Perkins, Reg. No. 33,027
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

TWP/lrs